Google Inc.
25 Massachusetts Avenue, N.W.
9th Floor
Washington, DC 20001

Main 202 346.1100
Fax 202 346.1101
www.google.com

September 26, 2016

Via ECFS

Brian Regan
Associate Bureau Chief
Wireless Telecommunications Bureau
Federal Communications Commission
445 Twelfth Street SW
Washington, DC 20554

Re: Proposal of Google for Certification as a SAS Administrator and ESC Operator; Supplemental Information (GN Docket 15-319)

Dear Mr. Regan:

This letter responds to your Request for Supplemental Information of September 2, 2016, regarding Google's proposal seeking certification to operate as a SAS Administrator and ESC operator in the 3550-3700 MHz Band (3.5 GHz Band).[1] Below, please find Google's responses to questions posed by the Commission.

1. **WTB/OET recently released a Public Notice establishing the final methodology for determining Grandfathered Wireless Protection Zones. Please update your proposal to describe how your SAS will protect Grandfathered Wireless Broadband Licensees accordingly. (pg.33) (§ 96.53(m))**

   In its recent Public Notice[2], the Commission adopted area protections within Grandfathered Wireless Protection Zones (GWPZ). All points within the zone will be protected to the same level as Priority Access License (PAL) Protection Areas (PPAs), namely -80 dBm per 10 MHz. The Public Notice does not provide a receive antenna height or other antenna characteristics, but we are presuming the intent is to use the same technical details employed for PPA protections, which are based on an isotropic receive antenna at 1.5 m AGL. The Wireless Innovation Forum (WinnForum) will establish standardized procedures for ensuring GWPZ protections, and Google will follow those industry-adopted standards. We describe here our concept for enforcing the GWPZs, but note that the details of how protections are ensured may evolve along with industry standards.

   When providing area protections, it is not enough to calculate aggregate interference at the closest boundary point, or at the boundary in general, because vertical geometry will

[1] Application of Google Inc. for Certification to Provide Spectrum Access System and Environmental Sensing Capability Services in GN Docket No. 15-319 (filed May 16, 2016) (Google Proposal).
[2] Public Notice, *Wireless Telecommunications Bureau and Office of Engineering and Technology Announce Methodology for Determining the Protected Contours for Grandfathered 3650-3700 MHz Band Licensees*, GN Docket 12-354 (rel. Aug. 19, 2016).

play an important role. For example, the boundary may be located at a low point, such as a riverbed, while potentially affected points interior to the GWPZ may be located on elevated terrain features, with few or no obstructions along the line of sight path from potential interferers. In this case, the signal strength at 1.5 m AGL may be higher at points interior to the GWPZ and more distant from the interference source, compared to points at the boundary that may be closer but lower. While the details are not finalized, initial discussions at the WinnForum have focused on computing aggregate interference levels over a set of representative sample points within the GWPZ. The SAS would use analysis sensitive to local conditions to select this set of points such that, within a small margin of error, aggregate interference at the selected points is the same as, or greater than, aggregate interference at nearby unsampled points within the GWPZ. This process should adequately capture the potential interference environment for Part 90 devices within the zone without causing excessive burden on the SAS.

2. **In the event that Google discontinues its operations as a SAS Administrator at the end of its term, describe how the SAS will securely transfer information to another approved entity at that time. This information includes all data relevant to SAS operation, such as IP addresses, URLs used to access its system, and a list of registered CBSDs. (§ 96.63(g))**

   Google has planned several features of its SAS to assure transfer of SAS operations to another SAS Administrator in the event that Google discontinues its SAS Administrator function.

   - The SAS-to-SAS interface would provide all content of the Google database to the SAS that is to take over management of the Google-managed devices. The current SAS-to-SAS interface is extensible to transfer the additional information that is not ordinarily exchanged with other SAS Administrators (such as billing information, device ownership, and network operator).

   - The Google SAS will operate behind a domain name that is not included within the Google DNS hierarchy (i.e., not an xxx.google.com domain) so that control of that domain can be transfered to another SAS Administrator, and references to the Google SAS can transition automatically to the new operator. Cutover would be accomplished by the new Administrator taking control over this domain name and providing its own SAS IP address in the associated DNS record.

   - Interactions with the SAS are through HTTPS requests (i.e., web requests). Upon cutover, requests to the Google SAS using the older resolved IP addresses would be redirected to the SAS taking responsibility for Google's CBSD clients. Any fully resolved IP addresses used in cached DNS records would be redirected to the new SAS Administrator until the changes in the DNS fully propagate through DNS system and are resolved by devices. Google would ensure forwarding of these SAS access requests until such time as the worst-case DNS propagation time is reached.

   - Google will use SAS Administrator certificates that are globally recognized by the SAS ecosystem, that is, certificates defined by the WinnForum cryptography

policy[3] and issued by approved Certificate Authorities. This ensures that devices that accept the Google certificates will also accept the certificates of the SAS Administrator that is taking over the management of Google registered devices.

- In the event that Google discontinues SAS operations, Google will transfer control of its ESC network to another SAS Administrator, or disable reporting by its ESC devices.

3. Describe how the SAS will operate without connectivity to sensitive military or federal databases. (§96.63(n)(1))

Google's SAS will protect federal incumbents without connectivity to any sensitive federal databases, as required by the rules. We will accomplish this by using our ESC network, as described in our Proposal, to detect federal incumbent activity.[4] The ESC network will alert the SAS to incumbent activity, and the SAS will use this information to protect incumbent operations as described in our response to question (9) below.

Until Google's ESC network is deployed, we will protect federal incumbents by enforcing the NTIA-defined coastal exclusion zones.

In neither case will Google connect to a sensitive military or federal database to accomplish federal incumbent protections. Note, however, that as described in our response to Question 10, below, Google will connect to those federal databases that are required by the rules, such as the FCC's Universal Licensing System and the FCC's list of incumbent FSS earth stations that require protection, for the purpose of protecting non-federal incumbents.[5]

4. Describe whether the SAS will permit CBSD operations in excess of the protection levels specified in Section 96.17 when an authorized user of a CBSD and a FSS earth station licensee mutually agree to such operation. If the SAS will permit excessive CBSD emissions upon mutual agreement, please discuss how the SAS will obtain the terms of this agreement and how it will communicate the terms promptly to other SAS Administrators. (§ 96.17(e))

Upon mutual agreement between Google and a the operator of a protected station, the Google SAS will permit alternative protection requirements. The Google SAS will also permit mutually agreed alternative protection requirements for which it has received notice from another SAS Administrator. If Google makes such agreements with an FSS earth station operator, Google will use the agreed exception management framework

[3] CBRS Communications Security Technical Specification, Document WINNF-15-S-0065, Version V1.0.0 (Aug. 2, 2016), *available at* http://www.wirelessinnovation.org/specifications.
[4] Google Proposal at Section 4.
[5] *See* 47 C.F.R. § 96.17(a). The sites are listed on the Commission's website at https://www.fcc.gov/general/35-ghz-band-protected-fixed-satellite-servicefss-earth-stations.

standardized by WinnForum[6] to promptly inform other SASs of the negotiated agreement, including relevant technical details.

5. **Describe how the SAS's authorization protocols for Category B CBSD operations will differ from the authorization protocols for Category A CBSD operations. (pgs. 7; 18-19) (§ 96.15(a))**

   In the registration process, all CBSDs need to provide the category of the CBSD antenna, the height (AGL or AMSL) of the antenna, and whether the antenna is deployed indoors or outdoors. The Google SAS will then verify that the information provided is consistent with the CBSD category. In addition, during registration, Category B CBSDs will be required to provide additional device-specific information including antenna azimuth, antenna downtilt, peak antenna gain, and antenna beamwidth. The registration process will fail if any required information is missing.

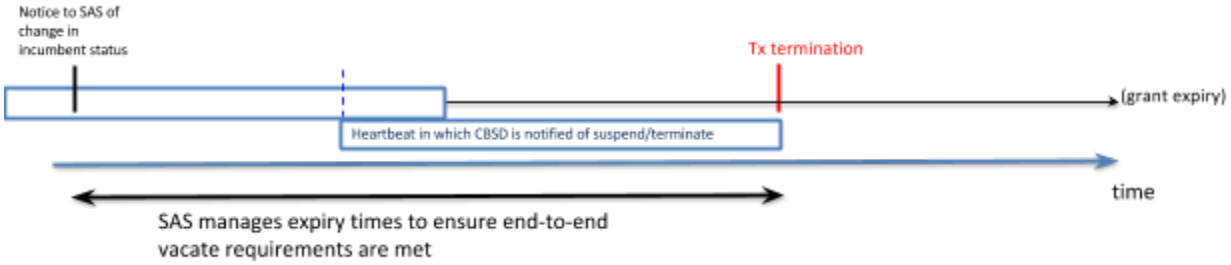
   In the time before the Google SAS has access to information from an approved ESC network, the Google SAS will authorize only Category A CBSDs outside the exclusions zones to transmit in 3550-3650 MHz. The Google SAS will not authorize Category B CBSDs to transmit in 3550-3650 MHz. Once the Google SAS obtains information on specific restricted areas and channels requiring protection from approved ESC devices, the Google SAS will authorize Category A and Category B CBSDs to transmit in channels and areas which do not require protection.

6. **Describe how the SAS will confirm the suspension or relocation of a CSBD operating within the same frequency as a federal incumbent, including the timeline within this process for CSBD suspension or relocation. (pgs. 6; 11) (§ 96.15(b)(4); 96.39(c)(2))**

   CBSDs receiving transmission authorization from the Google SAS will use the SAS-CBSD protocol currently being defined by WinnForum.[7] We expect that this protocol will require CBSDs to regularly contact the SAS for re-authorization (such contacts are called "heartbeats"). If an authorization request is unsuccessful, the CBSD will cease transmission. The SAS is responsible for managing the authorization extension times so as to maintain the invariant that CBSDs will suspend operations and/or relocate operations in the event of a federal incumbent utilizing the band.

   This process is illustrated in the figure below.

[6] *See* Item R1-SAD-03 in CBRS Operational and Functional Requirements, Document WINNF-15-S-0112, Version V1.0.0 (May 12, 2016), *available at* http://www.wirelessinnovation.org/specifications.
[7] When finalized, the protocol will be described in Document WINNF-16-S-0016, which will be available at http://www.wirelessinnovation.org/specifications.



"Tx termination" in the figure refers to the expiration of the continuing transmission authorization, which is renewed in every heartbeat request (the heartbeat request periods are shown in blue boxes), including any 60 second time allocated for ceasing transmission. Note that even in the event of a SAS-CBSD communication outage, the fail-safe nature of the protocol ensures that the CBSD does not violate any vacate requirements for use of the band.

Google expects that in many cases CBSD operators will choose to relocate operations to other channels not impacted by the presence of a federal incumbent. The SAS-CBSD protocol allows for the SAS to provide guidance to CBSDs about available channels in such cases.

7. **Discuss in more detail how the ESC controller will detect federal incumbent signals; please include the signal processing algorithms used by the ESC controller. (pg. 55) (*SAS / ESC Proposal PN*)**

   Confidential response filed separately under seal.

8. **Does Google acknowledge that the Commission, upon request, will review SAS fees and can require changes to those fees if they are found to be unreasonable? (pg. 16) (§ 96.65(b))**

   Yes. Consistent with Commission Rule 96.65, Google will charge CBRS users a reasonable fee for its provision of Subpart F SAS services.[8] Google acknowledges that the Commission may review those fees and can require changes if the fees are found to be unreasonable.

9. **Regarding the SAS's protocols for determining interference levels to sensitive and military incumbents, please describe how your model will calculate the signal strength and location information of those federal incumbents with indirect information from DoD/NTIA, particularly with respect to sensitive or military radar operations. (pgs. 18-25; 38-53) (§ 96.15)**

   Consistent with DoD expectations, our ESC network and SAS will not know the location of federal incumbents to a high degree of accuracy. Although specific requirements have not yet been provided by the DoD, we anticipate that an ESC sensor will report a quantized value of radar signal strength. Based upon the propagation model assumed for path loss between the radar and the sensor, and the assumed peak EIRP of the radar,

[8] 47 C.F.R. § 96.65.

this quantized signal strength will result in a radial distance uncertainty Δd from the ESC sensor node to the radar. An azimuthal uncertainty Δϕ will also be created, due to the ESC sensor antenna having a broad horizontal beamwidth. For example, the antennas planned for use in Google's ESC sensors have horizontal beamwidths of 90 degrees.

The combination of Δd and Δϕ will create a large area of uncertainty in the location of the incumbent radar. For example, with a 90 degree horizontal beam, and a radar that is located at some distance between 40 and 60 km of the ESC sensor node, the uncertainty area is some 1570 km^2. Within this large uncertainty zone, we will refine the possible location of the incumbent radar by taking into account the water depth. Since all of the non-land-based radars are located aboard aircraft carriers or large amphibious assault ships, the incumbent activity can only occur when the ships are in water with a depth (at high tide) equivalent to the minimum draft depth of this category of ships. Subject to concurrence by the Navy, we anticipate using 25 ft draft as our criterion. Close to shore, where the incumbent ship is likely to be visually apparent to the general public, this refinement will likely create significant constraints on the location of the incumbent activity (for example, at the pier or within an established shipping channel). Farther from the coast, in open water, this constraint is likely to have little effect in refining the radar location.

The SAS will compute co-channel interference to the incumbent radar using worst-case analysis within the possible zone of operation of the radar and will reconfigure CBSDs such that the radar's interference criteria will not be exceeded. The specific criterion that will be used is that specified in requirement R2-IPM-01of the WinnForum's technical standard WINNF-15-S-0112,[9] which was developed in conjunction with the DoD. (This requirement translates to -106 dBm/MHz receiver protection level within the detection area of uncertainty.)

The algorithm to be used will be similar to the representative sample point method used for PPA and GWPZ protection described in the answer to Question 1: for protecting large areas of uncertainty located mainly in uniform maritime conditions, a relatively small number of near-shore sample points will be adequate to ensure protection of the entire area of uncertainty. A very similar method was used by NTIA in defining the Exclusion Zones.[10]

10. Please explain how the SAS will access the Commission's database. (pgs. 4-8) (§ 96.55(d))

The Commission has made its ULS and IBFS databases available to the public, and the Google SAS will access required information contained in those databases related to FSS earth stations and Part 90 grandfathered stations requiring protection. Google has

[9] CBRS Operational and Functional Requirements, Document WINNF-15-S-0112, Version V1.0.0 (May 12, 2016), *available at* http://www.wirelessinnovation.org/specifications.

[10] *See* 47 C.F.R. 96.15(3) and National Telecommunications and Information Administration, *NTIA Technical Report TR-15-517: 3.5 GHz Exclusion Zone Analyses and Methodology* (June 18, 2015), *available at* http://www.ntia.doc.gov/report/2015/35-ghz-exclusion-zone-analyses-and-methodology.

contributed code demonstrating the retrieval and parsing of those database sources to a common testing and interop repository managed by WinnForum.

The Google SAS depends on several other FCC data sources, including the description of FSS earth stations qualifying for in-band SAS protection below 3700 MHz[11] and the description of the geographical borders between the United States and Canada and between the United States and Mexico.[12] Other, future FCC data may be used as well, such as databases governing CBRS operation near the borders, a one-time compilation of qualified Part 90 grandfathered base stations and associated protection region radii, a procedure for identifying FSS TT&C earth stations qualifying for out-of-band protection, and a mechanism for retrieving, by FCC ID from the equipment authorization database, the qualified CBRS equipment is authorized to transmit in the band.

Non-FCC Government data sources upon which the Google SAS relies include the geographical description of the census tracts in the United States, as maintained by the Census Department;[13] the geographical description of coastal and inland exclusion zones, as maintained by NTIA;[14] and terrain databases used for propagation modeling, as maintained by the U.S. Geological Survey.[15]

None of these publicly available, Government data sources are sensitive military or federal databases. Google understands that the future FCC-maintained data sources described above will also be developed with an aim towards making them available to the general public.

* * * * *

Please contact me should you have any questions about these responses to your inquiry.

Respectfully submitted,

Stephanie Selmer
Associate Corporate Counsel

cc: Paul Powell
Becky Schwartz
Ira Keltz

---

[11] *See* 47 C.F.R. § 96.17(a). The sites are listed on the Commission's website at https://www.fcc.gov/general/35-ghz-band-protected-fixed-satellite-servicefss-earth-stations.

[12] The files describing the geographical borders used by the Commission are available at https://transition.fcc.gov/oet/info/maps/uscabdry/uscabdry.zip and http://www.ibwc.gov/GIS_Maps/downloads/us_mex_boundary.zip.

[13] United States Census Bureau, *Tiger/Line Shapefiles and Tiger/Line Files*, *available at* https://www.census.gov/geo/maps-data/data/tiger-line.html (last visited Sept. 26, 2016).

[14] National Telecommunications and Information Administration, *3550-3650 MHz*, *available at* http://www.ntia.doc.gov/category/3550-3650-mhz.

[15] The terrain databases have not yet been published by the U.S. Geological Survey.